Quantum Mutual Authentication Scheme Based on Bell State Measurement

Muneer Alshowkan, *IEEE Student Member* and Khaled Elleithy, *IEEE Senior Member*
Department of Computer Science and Engineering
University of Bridgeport
Bridgeport, CT 06604, USA
malshowk@my.bridgeport.edu, elleithy@bridgeport.edu

***Abstract*—Authentication is one of the security services that ensures sufficient security of the system by identification and verification. Also, it assures the identity of the communicating party to be that the claimed one. To build a quantum channel between two unauthenticated to each other parties, first, a trusted authority is needed to establish a mutual authentication with each party. Using Bell measurement and entanglement swapping, we present a protocol that mutually authenticates the identity of the sender and the receiver, then constructs a quantum channel based on Bell basis. After, the sender and the receiver use the quantum channel to communicate using entanglement-assisted quantum communication protocols. Additionally, the protocol renews the shared secret key between the trusted authority and each user after each authentication process. The protocol provides the necessary authentication and key distribution to create a quantum channel between the sender and receiver.**

Keywords— quantum; entanglement; authentication; bell measurement; bell basis

I. Introduction

The field of quantum computing and information processing uses the laws of quantum physics, including states superposition and entanglement. Quantum cryptography is amongst the most surprising application of quantum mechanics in quantum computing and information processing. Unlike classical cryptography, which depends on the computational complexity of solving difficult mathematical problems such as, the public-key algorithm of the RSA. Quantum key distribution offers a method of sharing a private key with unconditional security. By applying the laws of quantum mechanics, messages and secret keys can be hidden and securely shared over a quantum channel between a sender and a receiver. For instance, one can use quantum key distribution protocols to share secret keys or use quantum direct communication to send messages. Bennett and Brassard were the first to propose the quantum key distribution protocol BB84 in 1984 [1]. After, the field of quantum computing and information processing became an active research area. Thus, many protocols in quantum communication and information processing have been proposed. For example, some of the quantum protocols are quantum secret sharing [2-8], quantum secure direct communication [9-14] and quantum identity authentication [13, 15-20]. Quantum secret sharing is the transformation of classical secret sharing to quantum information processing and, it can be used classical and quantum messages. Quantum secure direct communication protocol provides a secure method to send a secret message without prior sharing of a secret key. Classical cryptography has an extensive research on identity and message authentication. In the field of quantum information processing, quantum identity authentication is the natural generalization of the classical authentication. For instance, the quantum authentication and key distribution protocol presented in [16]. Identity authentication and simultaneous secret key distribution protocol presented in [21]. In addition, two protocols were presented in [13] for quantum user identification and secure direct communication. The protocols use the Greenberger-Horne-Zeilinger states for authentication and then secure communication.

One of the most fundamental elements of quantum cryptography is quantum entanglement. Quantum entanglement has no classical counterpart, which is a nonlocal correlation between two quantum subsystems. In 1991, Ekert [22] presented the first entanglement-based quantum key distribution protocol to share private secret keys. For example, if Alice and Bob have many prior shared maximally entangled pairs, then for each pair they perform measurement in any bases. After, on the classical channel they disclose the measurement basis used on each pair. The results should be correlated if they used the same basis. Pairs measured in different bases can be used to detect the presence of Eve by Bell's inequality. Entrapment swapping [23, 24] is a technique that makes two non-directly interacted systems entangled with each other. Using entanglement swapping led to presenting new quantum key distribution protocol [25-30].

In this paper, we assume that a sender (Alice) wishes to communicate with a receiver (Bob) but they are untrusted to each other and do not have access to a quantum channel nor they share entanglement. So, Alice contacts the trust authority Trent, who can authenticate each user using a prior shared secret key between them. Trent will distribute many two-particle entangled pairs with each party for authentication and communication. The goal is to verify and authenticate the identity of each user then, creates a quantum channel based on Bell basis. Trent renews the secret key between him and the users after each authentication. In the communication process, Alice and Bob use the entanglement-based quantum channel to communicate using entanglement-assisted communication protocol. The organization of the paper is as follows: the related work in section II, the proposed protocol in section III, the security analysis in section IV, and the conclusion in section V.

II. Related work

In the literature, there are different quantum authentication protocols [19, 31-33]. The protocols in [32, 33] are based on entanglement swapping and Bell state measurement. In addition, they have three participants in the protocols, a sender Alice, who wishes to communicate with a remote receiver Bob and Trent who is a trusted party. Trent will try to help and build an authenticated quantum communication channel between Alice and Bob. In the presented scheme registration, authentication and communication are the three main components. Next, we review the scheme presented in [33]. The protocol has three processes, which are registration, authentication, and communication.

A. Registration:

Suppose that each of Alice and Bob shares m bits secret key with the trusted authority Trent. Alice and Trent share the secret key $K_{TA} = \{K_{TA}^1, K_{TA}^2, \dots, K_{TA}^m, \}$. Also, Bob and Trent share the secret key $K_{TB} = \{K_{TB}^1, K_{TB}^2, \dots, K_{TB}^m, \}$. The key distribution method was the quantum key distribution protocol in [27] to guarantee the unconditional security. Alice asks Trent to communicate with Bob. Then, Trent starts the authentication process by using the prior shared secret keys K_{TA} and K_{TB} with Alice and Bob respectively. For each secret key, Trent derives a set of bases from the bases $B_z = \{|0\rangle, |1\rangle\}$ and $B_x = \{|+\rangle, |-\rangle\}$ for Alice and Bob called secret bases S_A and S_B respectively. Where, the bases B_z and B_x correspond to the secret key $i - th$ bit of "0" and "1" respectively. Trent authenticates the identity of Alice and Bob by creating and sending a random secret sequence encoded by the secret bases. For Alice, Trent creates:

$$S_{TA}^m = \{s_{TA}^1, s_{TA}^2, \dots s_{TA}^m\} \tag{1}$$

and for Bob, Trent creates:

$$S_{TB}^m = \{s_{TB}^1, s_{TB}^2, \dots s_{TB}^m\} \tag{2}$$

If Alice and Bob are the legitimate users, then they can use their shared secret key with Trent to derive the secret bases and decode the secret sequence. Therefore, Trent meets with each user on the classical channel to verify the result. They continue the protocol if both got the correct secret sequences or abandon the channel if one of them got the wrong result.

B. Authentication:

After the authentication of Alice and Bob identities, Trent starts building the quantum channel. Trent aims to create a quantum channel consists of two-particle maximally entangled states $\{|\Psi^{\pm}\rangle, |\Phi^{\pm}\rangle\}$. So, Trent prepares L maximally entangled pairs shared between him and Alice:

$$|\delta_{\mathrm{TA}}(i)\rangle = \{|\delta_{\mathrm{TA}}(1)\rangle, |\delta_{\mathrm{TA}}(2)\rangle, \dots |\delta_{\mathrm{TA}}(L)\rangle\} \tag{3}$$

also, another L pair shared between him and Bob:

$$|\zeta_{\mathrm{TB}}(j)\rangle = \{|\zeta_{\mathrm{TB}}(1)\rangle, |\zeta_{\mathrm{TB}}(2)\rangle, \dots |\zeta_{\mathrm{TB}}(L)\rangle\} \tag{4}$$

where $|\delta, \zeta\rangle \in \{|\Psi^{\pm}\rangle, |\Phi^{\pm}\rangle\}$. After, Trent keeps his particles which $|\delta_{\mathrm{T}}(i)\rangle$ and $|\zeta_{\mathrm{T}}(j)\rangle$. Then, he sends the particles $|\delta_{\mathrm{A}}(i)\rangle$ and $|\zeta_{\mathrm{B}}(j)\rangle$ to Alice and Bob respectively. Trent makes another authentication by asking each party to perform Bell basis measurement on k random pairs. For instance, if the chosen random state is r then Bell measurement should be performed on $|\delta_{\mathrm{A}}(r)\rangle|\delta_{\mathrm{A}}(r+1)\rangle$ and $|\zeta_{\mathrm{B}}(r)\rangle|\zeta_{\mathrm{B}}(r+1)\rangle$ for Alice and Bob respectively. After that, each party meets Trent on the classical channel to inform him of the chosen states and the measurements result. Trent verifies that the results of each party confirm the entanglement swapping of Bell states by performing Bell basis measurement on the chosen states. Trent continues the protocol if both parties obtained correct states.

C. Communication:

After successfully authenticated Alice and Bob, Trent is ready to create the quantum channel. First, Trent discards the used entanglement and asks Alice and Bob to discard them as well. The total remaining states in Trent possession will be $\{|\delta_{\mathrm{T}}(i)\rangle, |\zeta_{\mathrm{T}}(j)\rangle\}$ where $i = j = 1,2,..L - K$. Also, the remaining states in the possession of Alice and Bob will be $\{|\delta_{\mathrm{A}}(i)\rangle\}$ and $\{|\zeta_{\mathrm{B}}(j)\rangle\}$ respectively where $i = j = 1,2,..L - K$. After, Trent performs Bell basis measurement on the remaining states shared between him each party where $(i = j)$. For instance, Trent performs Bell basis measurement on $\{|\delta_{\mathrm{T}}(i)\rangle \otimes |\zeta_{\mathrm{T}}(j)\rangle\}$ which will cause entanglement swapping making the states of Alice and Bob $\{|\delta_{\mathrm{A}}(i)\rangle, |\zeta_{\mathrm{B}}(j)\rangle\}$ in one of Bell entangled states. Finally, Alice and Bob use an entanglement-assisted communication protocol such as quantum teleportation for communication.

The protocol presented in [34] is a bidirectional quantum secure direct communication with authentication. The communication channel between the sender Alice and the receiver Bob is based on two-particle prior shared entanglement. Alice and Bob encode their secret key and the secret message by Pauli operators σ_I, σ_X, σ_Z, and σ_Y. Also, they use the shared entanglement for authentication and secret key generating with help of $2N$ and $2M$ bits of classical communication. Moreover, Alice and Bob previously agree to encode the two bits $00,01,10$, and 11 with Pauli operators $\sigma_I, \sigma_X, \sigma_Z$, and σ_Y respectively:

$$\sigma_I = |0\rangle\langle 0| + |1\rangle\langle 1| \tag{5}$$

$$\sigma_X = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{6}$$

$$\sigma_Z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{7}$$

$$\sigma_Y = |0\rangle\langle 1| - |1\rangle\langle 0| \tag{8}$$

The protocol has eight steps. First, Alice prepares $2N + 2M' + \delta$ entangled pairs chosen randomly from Bell states then, shares them with Bob. Second, Bob randomly selects δ states from his entangled states then randomly measures them in σ_X *or* σ_Z. After, Bob informs Alice of the chosen state and their results through the classical channel. After that, Alice performs the same measurement on the same state then compares them with the results received from Bob. Third, using the remaining entanglement Alice encodes a secret key. Fourth, Bob perform measurement on the chosen state by Alice then announce the result through the classical channel. Fifth, Alice informs Bob of the position of the secret key states so, Bob perform the necessary decoding. Six, Alice encodes the secret message using the secret key. Seven, Bob perform Bell measurement then confirms with Alice the results through the classical channel. Eight, Alice informs Bob of the state of the direct communication and the updated authentication key. They use the direct communication states to send secret messages using Bell basis measurement.

III. Quantum Mutual Authentication Scheme Based on Bell State Measurement

The previous protocols especially [32, 33] do not offer mutual authentication and depend on the trusted authority to authenticate the users. Without mutual authentication, the communicating parties have no confidence they are connected with the trusted authority. Therefore, attacks such as replay and man-in-the-middle are possible. In our proposed protocol, we secure the registration process by mutual authentication. Also, renews the secret key after each use by distributing a new secret key after each successful authentication.

A. Mutual Authentication and Registration:

Consider a network of n users u_i where i is the user identification number $u_i \in U = \{u_1, u_2, \dots, u_n\}$. Each user shares a secret key $k_{Tu}^{2m} \in K = \{k_{Tu}^1, k_{Tu}^2, \dots, k_{Tu}^{2m}\}$ of size $2m$ where $k_{Tu}^{2m} = \{k_{Tu1}^m + k_{Tu2}^m\}$ with the trusted user Trent. We assume that the key exchange occurred during the setup of each user in the network. If Alice wishes to communicate with Bob, then she contacts Trent who knows every user in the network. At the beginning, Trent and Alice need to build mutual authentication by identification and verification of each's identity. They use the shared secret key $k_{TA}^{2m} = \{k_{TA1}^m + k_{TA2}^m\}$ to derive the encoding bases $b_{TA}^{2m} = \{b_{TA1}^m + b_{TA2}^m\}$ from the bases $B_z = \{|0\rangle, |1\rangle\}$ and the bases $B_x = \{|+\rangle, |-\rangle\}$. For each bit in the secret key, they make the bits "0" and "1" correspond to bases B_z and B_x respectively. After, Trent and Alice each generate a random sequence S_{TA} and S_{AT} respectively of size m, then encoded it by the bases b_{TA1}^m. Next, Trent and Alice exchange the encoded sequences. So, the legitimate Trent and Alice must be able to derive the decoding bases b_{TA1}^m from the secret key k_{TA1}^m then decode the each other's sequence. After, they meet on the classical channel. Trent announces Alice's S_{AT}^m and Alice announces Trent's sequence S_{TA}^m. Trent and Alice verify their sequences then, they continue if they received the correct sequences so that they are mutually authenticated. If one of them received the wrong sequence then, they abandon the channel. After that, Trent contacts Bob and performs the same authentication process. Trent and Bob use the shared secret key $k_{TB}^{2m} = \{k_{TB1}^m + k_{TB2}^m\}$ to derive the encoding bases $b_{TA}^{2m} = \{b_{TB1}^m + b_{TB2}^m\}$. Next, Each of Trent and Bob generates a random sequence S_{TB}^m and S_{BT}^m respectively of size m then, encode it by bases b_{TB1}^m. After, Trent and Bob exchange the encoded sequences then meet on the classical channel to verify their sequences. Trent and Bob verify the sequences S_{TB}^m and S_{BT}^m respectively then, they continue if both received the correct sequences or they abandon the channel. If no one abandoned the channel then, Trent and Alice, as well as Trent and Bob, are mutually authenticated. Further, Trent will provide Alice and Bob with a secret key to create a secret sequence for authenticating before communication. Trent encodes the second part of Bob's secret key k_{TB2}^m by b_{TA2}^m then sends it to Alice. Also, Trent encodes the second part of Alice's secret key k_{TA2}^m using b_{TB2}^m then sends to Bob.

B. Secret Key Distribution:

Trent builds the quantum channel after he created the mutual authentication between him and each of Alice and Bob. For each user, Trent prepares L random Bell basis:

$$|\Upsilon(L)\rangle_{Tu} = \{|\Upsilon(1)\rangle_{Tu}, |\Upsilon(2)\rangle_{Tu}, \dots, |\Upsilon(\mathrm{L})\rangle_{Tu}\} \quad (9)$$

where $|\Upsilon\rangle \in \{|\Psi^-\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Phi^+\rangle\}$ then shares them with the user. Also, let i and j be the indexes of Alice and Bob states respectively where $i = j = t + q + p = L$. Trent shares the entangled pairs $|\Upsilon(i)\rangle_{TA}$ with Alice by keeping the first particle of $|\Upsilon(i)\rangle_T$ and sending the second particle $|\Upsilon(i)\rangle_A$ to Alice. Likewise, Trent shares the entangled pairs $|\Upsilon(j)\rangle_{TB}$ with Bob by keeping the first particles $|\Upsilon(j)\rangle_T$ and sending the second particle $|\Upsilon(j)\rangle_B$ to Bob. After, Alice randomly chooses $(t+q)/2$ inconsecutive states of her entanglement with Trent $|\Upsilon(L)\rangle_{TA}$ then performs Bell measurement on the state $|\Upsilon(i)\rangle_{TA} \otimes |\Upsilon(i+1)\rangle_{TA}$. For example, if the random state i is $|\Phi^+(i)\rangle_{12}$ and the state $i+1$ is $|\Phi^+(i+1)\rangle_{34}$ where the particles 1 and 4 belong to Trent and the particles 2 and 3 belong to Alice. Then, Bell measurement on $|\Phi^+\rangle_{12} \otimes |\Phi^+\rangle_{34}$ will give one result of $\{|\Phi^+\rangle_{14}|\Phi^+\rangle_{23}\}$, $\{|\Phi^-\rangle_{14}|\Phi^-\rangle_{23}\}$, $\{|\Psi^+\rangle_{14}|\Psi^+\rangle_{23}\}$, or $|\Psi^-\rangle_{14}|\Psi^-\rangle_{23}$ each occurs with a probability of $1/4$. If Alice finds the state $|\Psi^+\rangle_{23}$ then the state Trent holds should be $|\Psi^+\rangle_{14}$. All the possible outcomes of Bell measurement when the state i equals to Bell state $|\Phi^+\rangle_{12}$ are:

$$\Phi_{12}^+ \otimes \Phi_{34}^+ = \Phi_{14}^+\Phi_{23}^+, \Phi_{14}^-\Phi_{23}^-, \Psi_{14}^+\Psi_{23}^+, \Psi_{14}^-\Psi_{23}^- \quad (10)$$

$$\Phi_{12}^+ \otimes \Phi_{34}^- = \Phi_{14}^+\Phi_{23}^-, \Phi_{14}^-\Phi_{23}^+, \Psi_{14}^+\Psi_{23}^-, \Psi_{14}^-\Psi_{23}^+ \quad (11)$$

$$\Phi_{14}^+ \otimes \Psi_{34}^+ = \Phi_{14}^+\Psi_{23}^+, \Phi_{14}^-\Psi_{23}^-, \Psi_{14}^+\Phi_{23}^+, \Psi_{14}^-\Phi_{23}^- \quad (12)$$

$$\Phi_{12}^+ \otimes \Psi_{34}^- = \Phi_{14}^+\Psi_{23}^-, \Phi_{14}^-\Psi_{23}^+, \Psi_{14}^+\Phi_{23}^-, \Psi_{14}^-\Phi_{23}^+ \quad (13)$$

If the state i equals to $|\Phi^-\rangle_{12}$, then all the possible outcomes of Bell measurement are:

$$\Phi_{12}^- \otimes \Phi_{34}^- = \Phi_{14}^+\Phi_{23}^+, \Phi_{14}^-\Phi_{23}^-, \Psi_{14}^+\Psi_{23}^+, \Psi_{14}^-\Psi_{23}^- \quad (14)$$

$$\Phi_{12}^- \otimes \Psi_{34}^- = \Phi_{14}^+\Psi_{23}^+, \Phi_{14}^-\Psi_{23}^-, \Psi_{14}^+\Phi_{23}^+, \Psi_{14}^-\Phi_{23}^- \quad (15)$$

$$\Phi_{12}^- \otimes \Phi_{34}^+ = \Phi_{14}^+\Phi_{23}^-, \Phi_{14}^-\Phi_{23}^+, \Psi_{14}^+\Psi_{23}^-, \Psi_{14}^-\Psi_{23}^+ \quad (16)$$

$$\Phi_{12}^- \otimes \Psi_{34}^+ = \Phi_{14}^+\Psi_{23}^-, \Phi_{14}^-\Psi_{23}^+, \Psi_{14}^+\Phi_{23}^-, \Psi_{14}^-\Phi_{23}^+ \quad (17)$$

If the state i equals to $|\Psi^+\rangle_{12}$, then all the possible outcomes of Bell measurement are:

$$\Psi_{12}^+ \otimes \Psi_{34}^+ = \Phi_{14}^+\Phi_{23}^+, \Phi_{14}^-\Phi_{23}^-, \Psi_{14}^+\Psi_{23}^+, \Psi_{14}^-\Psi_{23}^- \quad (18)$$

$$\Psi_{12}^+ \otimes \Psi_{34}^- = \Phi_{14}^+\Phi_{23}^-, \Phi_{14}^-\Phi_{23}^+, \Psi_{14}^+\Psi_{23}^-, \Psi_{14}^-\Psi_{23}^+ \quad (19)$$

$$\Psi_{12}^+ \otimes \Phi_{34}^+ = \Phi_{14}^+\Psi_{23}^+, \Phi_{14}^-\Psi_{23}^-, \Psi_{14}^+\Phi_{23}^+, \Psi_{14}^-\Phi_{23}^- \quad (20)$$

$$\Psi_{12}^+ \otimes \Phi_{34}^- = \Phi_{14}^+\Psi_{23}^-, \Phi_{14}^-\Psi_{23}^+, \Psi_{14}^+\Phi_{23}^-, \Psi_{14}^-\Phi_{23}^+ \quad (21)$$

If the state i equals to $|\Psi^-\rangle_{12}$, then all the possible outcomes of Bell measurement are:

$$\Psi_{12}^- \otimes \Psi_{34}^- = \Phi_{14}^+\Phi_{23}^+, \Phi_{14}^-\Phi_{23}^-, \Psi_{14}^+\Psi_{23}^+, \Psi_{14}^-\Psi_{23}^- \quad (22)$$

$$\Psi_{12}^- \otimes \Psi_{34}^+ = \Phi_{14}^+\Phi_{23}^-, \Phi_{14}^-\Phi_{23}^+, \Psi_{14}^+\Psi_{23}^-, \Psi_{14}^-\Psi_{23}^+ \quad (23)$$

$$\Psi_{12}^- \otimes \Phi_{34}^- = \Phi_{14}^+\Psi_{23}^+, \Phi_{14}^-\Psi_{23}^-, \Psi_{14}^+\Phi_{23}^+, \Psi_{14}^-\Phi_{23}^- \quad (24)$$

$$\Psi_{12}^- \otimes \Phi_{34}^+ = \Phi_{14}^+\Psi_{23}^-, \Phi_{14}^-\Psi_{23}^+, \Psi_{14}^+\Phi_{23}^-, \Psi_{14}^-\Phi_{23}^+ \quad (25)$$

For each measurement result, Alice will represent the states $|\Phi\rangle$ and $|\Psi\rangle$ by the bits "0" and "1" respectively. In the same manner, she represents the phase of the states " + " and " − " by the bits "0" and "1" respectively Fig. 1. For error detection, Alice meets with Trent on the classical channel to inform him of the $t/2$ chosen pairs and the measurement result of each pair. Trent verifies if the results Alice obtained satisfy Bell state measurement for the chosen $t/2$ pairs. If Trent finds the results do not satisfy Bell measurement then, the channel is compromised and they abandon the channel. However, if the results satisfy Bell measurement for entanglement swapping then, Trent and Alice represent the remaining $q/2$ pairs in bits and consider them as an initial secret key r.

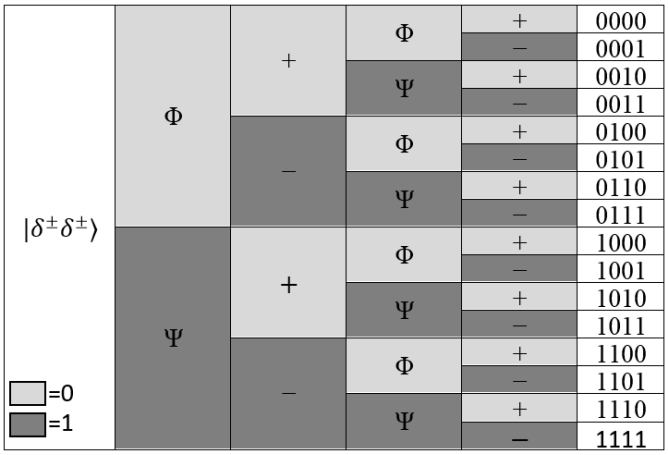

Fig. 1. The representation of the states using classical bits.

Let consider an attacker (Eve) listens to the classical channel and gains some information about the initial secret key. Then another level of security is needed to reduce Eve's information. Therefore, Trent and Alice apply privacy amplification to derive a secret key with a low correlation to the initial key. We assume that every user shares with Trent a family of universal hash function [35] GF with a uniform distribution of hash functions g which, maps n bits input A to m bits output B. Also, if $\{r_1, r_2\} \in A$ and g is randomly selected then, $g(r_1) = g(r_2)$ with probability of $1/|B|$. Trent selects a hash function $g \in GF$ then informs Alice through the classical channel which hash function was selected. After, Trent and Alice feed the initial secret key into the hash function to obtain the final secret key $g(r) = k_{TA}^m$. Similarly, Trent follows the same process of verification and key distribution with Bob to obtain a new secret key k_{TB}^m.

C. Communication:

Trent reorders the p remaining entangled pairs between him and Alice:

$$|\Upsilon(i)\rangle_{TA} = \{|\Upsilon(1)\rangle_{TA}, |\Upsilon(2)\rangle_{TA}, \dots, |\Upsilon(p)\rangle_{TA}\} \quad (26)$$

and the remaining p entangled pairs between him and Bob:

$$|\Upsilon(j)\rangle_{TB} = \{|\Upsilon(1)\rangle_{TB}, |\Upsilon(2)\rangle_{TB}, \dots, |\Upsilon(p)\rangle_{TB}\} \quad (27)$$

Then, Trent performs entanglements swapping to create entanglement state between Alice and Bob. Trent performs entanglement swapping process using $|\Upsilon(i)\rangle_{TA} \otimes |\Upsilon(j)\rangle_{TB}$. For example if the entangled state between Trent and Alice is $|\Upsilon(i)\rangle_{TA} = |\Phi^+\rangle_{TA}$ and the entangled state between Trent and Bob is $|\Upsilon(j)\rangle_{TB} = |\Phi^+\rangle_{TB}$ then $|\Phi^+(i)\rangle_{TA} \otimes |\Phi^+(j)\rangle_{TB}$ is as follows:

$$= \frac{|0\rangle_T|0\rangle_A + |1\rangle_T|1\rangle_A}{\sqrt{2}} \otimes \frac{|0\rangle_T|0\rangle_B + |1\rangle_T|1\rangle_B}{\sqrt{2}} \quad (28)$$

$$= \frac{1}{2}\begin{Bmatrix} |0\rangle_T|0\rangle_A\,(|0\rangle_T|0\rangle_B + |1\rangle_T|1\rangle_B) \\ +|1\rangle_T|1\rangle_A\,(|0\rangle_T|0\rangle_B + |1\rangle_T|1\rangle_B) \end{Bmatrix} \quad (29)$$

Trent applies CNOT gate on T using the forst T as the control and the second T as the target:

$$= \frac{1}{2}\begin{Bmatrix} |0\rangle_T|0\rangle_A\,(|0\rangle_T|0\rangle_B + |1\rangle_T|1\rangle_B) \\ +|1\rangle_T|1\rangle_A\,(|1\rangle_T|0\rangle_B + |0\rangle_T|1\rangle_B) \end{Bmatrix} \quad (30)$$

Trent apples the Hadamard gate on the first T:

$$= \frac{1}{2\sqrt{2}}\begin{Bmatrix} (|0\rangle_T + |1\rangle_T)\,|0\rangle_A\,(|0\rangle_T|0\rangle_B + |1\rangle_T|1\rangle_B) \\ +(|0\rangle_T - |1\rangle_T)|1\rangle_A\,(|1\rangle_T|0\rangle_B + |0\rangle_T|1\rangle_B) \end{Bmatrix} \quad (31)$$

Rearranging and combining T:

$$= \frac{1}{2\sqrt{2}}\begin{Bmatrix} |00\rangle_T|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B \\ |01\rangle_T|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B \\ |10\rangle_T|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B \\ |11\rangle_T|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B \end{Bmatrix} \quad (32)$$

Trent informs Alice and Bob about which state they share using two classical bits. Therefore, Alice and Bob will have their i and j states respectively entangled in one of Bell states each occurring with probability of 1/4.

$$|\Psi^-(i,j)\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) \quad (33)$$

$$|\Psi^+(i,j)\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \quad (34)$$

$$|\Phi^-(i,j)\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \quad (35)$$

$$|\Phi^+(i,j)\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \quad (36)$$

Alice and Bob use their entangled pairs to communicate using quantum communication protocols such as teleportation, Ekert 91, or remote state preparation. Alice and Bob make final authentication to make sure that each party is the same party, Trent authenticated in the first process. They use the secret key k_{TA2}^m and k_{TB2}^m which, Trent distributed to Bob and Alice respectively. Each party derives the encoding basis, then creates and exchanges a secret sequence. After, Alice and Bob meet on the classical channel to verify each other's sequence. The legitimate Alice and Bob should be able to decode and verify their identity. If one of them cannot decode the sequence and verify their identity, then they cannot trust each other and abandon the channel. However, if they are the legitimate Alice and Bob then, they will be able to decode the sequences and have mutual authentication. So, Alice and Bob are authenticated to each other's and able to start the communication using the entanglement-assisted quantum communication protocols.

IV. Security Analysis and Discussion

Mutual authentication requires the communicating parties to build confidence about the identity of each other's by identification and verification. For comparison, the quantum authentication protocol in [33] does not authenticate Trent to the communicating parties Alice and Bob. The protocol assumes that Trent and each party share a secret, which then used by Trent to derive basis to encode a challenging sequence. Trent sends the encoded sequence and asks each party to decode it after deriving the decoding basis from their shared secret key with him. They retrieve the correct sequence then send the result to Trent to decide if they are the legitimate users or not. However, an attacker (Eve) can masquerades Trent without being detected by Alice and Bob because Trent uses the quantum channel to send encoded sequence and Alice and Bob use the classical channel to verify their identity. For example, Eve can intercept the communication between Alice and Trent then forge a verification process. Eve generates random secret key k_E^m then derives encoding basis b_E^m. After, Eve creates the sequence S_{EA}^m then, sends it to Alice. Using the secret key k_{TA}^m, Alice derives the basis b_{TA}^m then tries to decode the sequence S_{EA}^m. Without identity verification of the source of the sequence, Alice will send the result to Trent. However, Eve can intercept the communication from reaching Trent then continues with Bob because Trent is the only one performs the authentication. Even if Alice requests acknowledgement from Trent then, without authentication, Eve can perform the replay attack. Therefore, Alice and Bob also need to authenticate the identity of Trent at the initial communication. Alice and Bob each creates a sequence using the shared secret key with Trent then ask him to verify the sequence on the classical channel. Thus, Alice and Bob require Trent to verify himself and pass the verification step to be as well authenticated. If the mutual authentication succeeds then, Alice and Bob with high confidence can continue communicating with Trent because they have mutual authentication. If not, they abandon the channel. In our protocol, consider Eve tries to perform the replay attack. Using the passive attack on the classical channel, Eve could capture acknowledgements and use them later. However, the shared secret key in our protocol changes after each authentication process. Thus, each secret key is used once and the replay attack cannot be effective.

Let us consider the intercept/send attack against the authentication and key distribution process. If Eve intercepts the entangled pairs sent from Trent to Alice then, creates entanglement and share with Alice. So, Trent and Eve share $|\Upsilon(j)\rangle_{TE}$. Also, Eve and Alice share $|\Upsilon(j)\rangle_{EA}$. Alice chooses random pairs then, performs Bell measurement to obtain an outcome with a probability of 1/4 for each measurement as in Bell measurement outcomes (10-25). Similarly, Eve measures random pairs from the shared entanglement with Trent to obtain an outcome for each measurement with a probability of 1/4. When Alice meets Trent on the classical channel to inform him of the chosen pairs and their measurement results, Alice will not be able to provide the correct measurement because there is no correlation between their pairs. Therefore, each measurement result of Alice and Trent will have success probability of 1/16. As a result, Trent and Alice with high probability can detect the presence of Eve on the channel.

V. Conclusion

We presented a quantum mutual authentication protocol based on Bell state measurement and entanglement swapping. A trusted authority authenticates untrusted to each other users then creates an entanglement-based quantum communication channel. Using the prior shared secret key with each user, the trusted authority mutually authenticates each user then builds the quantum channel. In addition, the protocol renews the secret key shared with the trusted authority after each authentication process. The protocol successfully creates Bell states between parties who their particles did not interact with each other's before. Then, they use their Bell states to communicate by quantum entanglement communication protocols.

VI. References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984, p. 8.

[2] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Physical Review A,* vol. 59, p. 162, 1999.

[3] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, "Efficient multiparty quantum-secret-sharing schemes," *Physical Review A,* vol. 69, p. 052307, 2004.

[4] Z.-j. Zhang, Y. Li, and Z.-x. Man, "Multiparty quantum secret sharing," *Physical Review A,* vol. 71, p. 044301, 2005.

[5] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A,* vol. 59, p. 1829, 1999.

[6] Z.-j. Zhang, G. Gao, X. Wang, L.-f. Han, and S.-h. Shi, "Multiparty quantum secret sharing based on the improved Boström–Felbinger protocol," *Optics communications,* vol. 269, pp. 418-422, 2007.

[7] P. Zhou, X.-H. Li, Y.-J. Liang, F.-G. Deng, and H.-Y. Zhou, "Multiparty quantum secret sharing with pure entangled states and decoy photons," *Physica A: Statistical Mechanics and its Applications,* vol. 381, pp. 164-169, 2007.

[8] Y. Sun, Q.-y. Wen, F. Gao, X.-b. Chen, and F.-c. Zhu, "Multiparty quantum secret sharing based on Bell measurement," *Optics Communications,* vol. 282, pp. 3647-3651, 2009.

[9] C. Qing-Yu and L. Bai-Wen, "Deterministic secure communication without using entanglement," *Chinese Physics Letters,* vol. 21, p. 601, 2004.

[10] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Physical Review Letters,* vol. 89, p. 187902, 2002.

[11] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Physical Review A,* vol. 69, p. 052319, 2004.

[12] A. Beige, B. G. Englert, C. Kurtsiefer, and H. Weinfurter, "Secure communication with a publicly known key," *Acta Physica Polonica A,* vol. 101, pp. 357-368, 2002.

[13] H. Lee, J. Lim, and H. Yang, "Quantum direct communication with authentication," *Physical Review A,* vol. 73, p. 042305, 2006.

[14] Q.-Y. Cai and B.-W. Li, "Improving the capacity of the Boström-Felbinger protocol," *Physical Review A,* vol. 69, p. 054301, 2004.

[15] T. Mihara, "Quantum identification schemes with entanglements," *Physical review A,* vol. 65, p. 052326, 2002.

[16] M. Dušek, O. Haderka, M. Hendrych, and R. Myška, "Quantum identification system," *Physical Review A,* vol. 60, p. 149, 1999.

[17] Z. Zhang, G. Zeng, N. Zhou, and J. Xiong, "Quantum identity authentication based on ping-pong technique for photons," *Physics Letters A,* vol. 356, pp. 199-205, 2006.

[18] X. Zhang, "One-way quantum identity authentication based on public key," *Chinese Science Bulletin,* vol. 54, pp. 2018-2021, 2009.

[19] Y. Yang, Q. Wen, and X. Zhang, "Multiparty simultaneous quantum identity authentication with secret sharing," *Science in China Series G: Physics, Mechanics and Astronomy,* vol. 51, pp. 321-327, 2008.

[20] C.-H. Yu, G.-D. Guo, and S. Lin, "Quantum secure direct communication with authentication using two nonorthogonal states," *International Journal of Theoretical Physics,* vol. 52, pp. 1937-1945, 2013.

[21] G. Zeng and W. Zhang, "Identity verification in quantum key distribution," *Physical Review A,* vol. 61, p. 022303, 2000.

[22] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys Rev Lett,* vol. 67, pp. 661-663, Aug 5 1991.
[23] M. Zukowski, A. Zeilinger, M. Horne, and A. Ekert, "" Event-ready-detectors" Bell experiment via entanglement swapping," *Physical Review Letters,* vol. 71, pp. 4287-4290, 1993.
[24] L. Hardy and D. D. Song, "Entanglement-swapping chains for general pure states," *Physical Review A,* vol. 62, p. 052315, 2000.
[25] S. Bose, V. Vedral, and P. L. Knight, "Multiparticle generalization of entanglement swapping," *Physical Review A,* vol. 57, p. 822, 1998.
[26] A. Cabello, "Quantum key distribution in the Holevo limit," *Phys Rev Lett,* vol. 85, pp. 5635-8, Dec 25 2000.
[27] D. Song, "Secure key distribution by swapping quantum entanglement," *Physical Review A,* vol. 69, p. 034301, 2004.
[28] C. Li, H.-S. Song, L. Zhou, and C.-F. Wu, "A random quantum key distribution achieved by using Bell states," *Journal of Optics B: Quantum and Semiclassical Optics,* vol. 5, p. 155, 2003.
[29] G. Gao, "Quantum key distribution by swapping the entanglement of χ-type state," *Physica Scripta,* vol. 81, p. 065005, 2010.
[30] N. Zhou, L. Wang, L. Gong, X. Zuo, and Y. Liu, "Quantum deterministic key distribution protocols based on teleportation and entanglement swapping," *Optics Communications,* vol. 284, pp. 4836-4842, 2011.
[31] Y. Yu-Guang and W. Qiao-Yan, "Economical multiparty simultaneous quantum identity authentication based on Greenberger–Horne–Zeilinger states," *Chinese Physics B,* vol. 18, 2009.
[32] N. Penghao, C. Yuan, and L. Chong, "Quantum Authentication Scheme Based on Entanglement Swapping," *International Journal of Theoretical Physics,* pp. 1-11, 2015.
[33] M. Naseri, "Revisiting Quantum Authentication Scheme Based on Entanglement Swapping," *International Journal of Theoretical Physics,* pp. 1-8, 2015.
[34] D. Shen, W. Ma, X. Yin, and X. Li, "Quantum dialogue with authentication based on Bell states," *International Journal of Theoretical Physics,* vol. 52, pp. 1825-1835, 2013.
[35] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," in *Proceedings of the ninth annual ACM symposium on Theory of computing*, 1977, pp. 106-112.